

#2

EL896636889US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Hisao FURUKAWA, et al.)
Serial No.: not yet assigned)
Filed: Concurrently herewith)
For: "INTEGRATED INFORMATION) Our Ref: B-4235 618927-6
COMMUNICATION SYSTEM) Date: July 5, 2001

J1046 U.S. PTO
09/899404
07/05/01

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

Commissioner of Patents and Trademarks
Box New Patent Application
Washington, D.C. 20231

Sir:

[X] Applicants hereby make a right of priority claim under 35
U.S.C. 119 for the benefit of the filing date(s) of the
following corresponding foreign application(s):

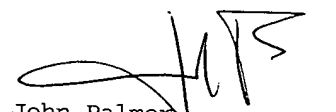
<u>COUNTRY</u>	<u>FILING DATE</u>	<u>SERIAL NUMBER</u>
JAPAN	12 July 2000	2000-211451
JAPAN	9 May 2001	2001-138298

[] A certified copy of each of the above-noted patent
applications was filed with the Parent Application
No. _____.

[X] To support applicants' claim, certified copies of the above-
identified foreign patent applications are enclosed herewith.

[] The priority document will be forwarded to the Patent Office
when required or prior to issuance.

Respectfully submitted,


John Palmer
Attorney for Applicant
Reg. No. 36,885

LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
Telephone: (323) 934-2300
Telefax: (323) 934-0202

日 本 国 特 許 庁
JAPAN PATENT OFFICE

J1046 U.S. PTO
09/899404
07/05/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2000年 7月12日

出 願 番 号
Application Number:

特願2000-211451

出 願 人
Applicant(s):

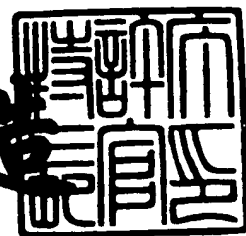
財団法人流通システム開発センター
有限会社宮口研究所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月30日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 RS0002

【提出日】 平成12年 7月12日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/60

【発明の名称】 統合情報通信システム

【請求項の数】 4

【発明者】

 【住所又は居所】 埼玉県川越市伊勢原町 2 - 2 7 - 7

 【氏名】 古川 久夫

【発明者】

 【住所又は居所】 千葉県市川市菅野 1 - 4 - 4

 【氏名】 宮口 庄司

【特許出願人】

 【持分】 006/010

 【識別番号】 596176286

 【氏名又は名称】 財団法人流通システム開発センター

【特許出願人】

 【持分】 004/010

 【識別番号】 398009317

 【氏名又は名称】 有限会社宮口研究所

【代理人】

 【識別番号】 100078776

 【弁理士】

 【氏名又は名称】 安形 雄三

【選任した代理人】

 【識別番号】 100087055

 【弁理士】

 【氏名又は名称】 鈴木 淳也

【選任した代理人】

【識別番号】 100084803

【弁理士】

【氏名又は名称】 村山 勝

【手数料の表示】

【予納台帳番号】 010836

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 統合情報通信システム

【特許請求の範囲】

【請求項 1】 通信会社管理網を含む統合情報通信システムであり、前記通信会社管理網はアクセス制御装置、中継装置及びサーバを含み、前記アクセス制御装置、中継装置及びサーバは相互に IP 通信回線で接続されており、前記通信会社管理網は境界中継装置を経て前記 IP 通信回線により接続されており、

前記統合情報通信システムの外部の端末はユーザ通信回線を経由して前記アクセス制御装置に接続され、前記ユーザ通信回線の終端の論理端子を識別するために、前記論理端子に内部アドレスが付与されると共に、前記アクセス制御装置は変換表を含み、

前記変換表の要求識別が仮想専用線を意味する場合、外部パケットが入力した論理端子の識別情報が定まれば、送信側のアクセス制御装置が生成する内部パケットのヘッダに格納する内部宛先アドレスが一意に定まるように前記変換表のレコードとして登録されており、

前記要求識別がプライベートアドレス通信を意味する場合、外部パケットが入力した論理端子の識別情報、外部ソースアドレス及び外部宛先アドレスの組が定まれば、前記送信側のアクセス制御装置が生成する内部パケットのヘッダに格納する内部宛先アドレスが一意に定まるように前記変換表のレコードとして登録されており、

同一の論理端子識別情報に対して、前記外部宛先アドレス及び前記ヘッダ部に格納する内部宛先アドレスの組が共にレコード毎に異なり、同一論理端子から入力する外部パケット内の外部宛先アドレスを変更することにより前記外部パケットの到達先を変更できるようになっており、

前記要求識別が非プライベートアドレス通信を意味する場合、前記論理端子識別情報及び外部ソースアドレスの組が前記変換表のレコードとして登録されており、当該登録は前記外部ソースアドレスを有する端末からの送信許可を意味し、前

記外部パケットが前記端末から前記ユーザ通信回線に送信され、前記外部パケットが入力した論理端子の識別情報を含む前記変換表のレコードに、前記要求識別が仮想専用線と登録されていることが検出され、前記変換表から取得した論理端子識別情報及び内部宛先アドレスを用いて前記外部パケットから前記内部パケットに変換され、

前記内部パケットは前記統合情報通信システム内部の前記IP通信回線及び中継装置を経由して転送され、受信側のアクセス制御装置の論理端子を経て他のユーザ通信回線を転送されて他の端末に到達するようになっており、

前記アクセス制御装置内のパケットフィルタは、外部パケット内の宛先アドレスが網外非公開アドレスであることを検出すると、前記外部パケットを廃棄するようになっていることを特徴とする統合情報通信システム。

【請求項2】 通信会社管理網を含む統合情報通信システムであり、前記通信会社管理網はアクセス制御装置、中継装置及びサーバを含み、前記アクセス制御装置、中継装置及びサーバは相互にIP通信回線で接続されており、

前記通信会社管理網は境界中継装置を経て前記IP通信回線により接続されており、

前記統合情報通信システムの外部の端末はユーザ通信回線を経由して前記アクセス制御装置に接続され、前記ユーザ通信回線の終端の論理端子を識別するために、前記論理端子に内部アドレスが付与されると共に、前記アクセス制御装置は変換表を含み、

前記変換表の要求識別が仮想専用線を意味する場合、外部パケットが入力した論理端子の識別情報が定まれば、送信側のアクセス制御装置が生成する内部パケットのヘッダに格納する内部宛先アドレスが一意に定まるように前記変換表のレコードとして登録されており、

前記要求識別がプライベートアドレス通信を意味する場合、外部パケットが入力した論理端子の識別情報、外部ソースアドレス及び外部宛先アドレスの組が定まれば、前記送信側のアクセス制御装置が生成する内部パケットのヘッダに格納する内部宛先アドレスが一意に定まるように前記変換表のレコードとして登録されており、

同一の論理端子識別情報に対して、前記外部宛先アドレス及び前記ヘッダ部に格納する内部宛先アドレスの組が共にレコード毎に異なり、同一論理端子から入力する外部パケット内の外部宛先アドレスを変更することにより前記外部パケットの到達先を変更できるようになっており、

前記要求識別がプライベートアドレス通信と登録されていることが検出されたとき、

前記外部パケット内の外部ソースアドレス及び外部宛先アドレスが共に前記変換表のレコードに登録されていることが検出されたとき、前記変換表から取得した論理端子識別情報及び内部宛先アドレスを用いて前記外部パケットから前記内部パケットに変換され、

前記要求識別が非プライベートアドレス通信と登録されていることが見出されたとき、

前記外部パケット内の外部ソースアドレスが前記変換表のレコードに登録されていれば、前記外部ソースアドレスを有する端末の送信許可を確認できたので、前記外部パケットをそのまま前記内部パケットとし、

前記内部パケットは前記統合情報通信システム内部のIP通信回線と中継装置を経由して転送され、受信側のアクセス制御装置の論理端子を経て他のユーザ通信回線を転送され、他の端末に到達するようになっており、

前記アクセス制御装置内のパケットフィルタは、前記外部パケット内の宛先アドレスが網外非公開アドレスであることを検出すると、この外部パケットを廃棄するようになっていることを特徴とする統合情報通信システム。

【請求項 3】 前記通信会社管理網間の前記 IP パケットの送受信は通信会社間に共通のアドレスを用い、境界中継装置のパケットフィルタは、前記外部パケット内の宛先アドレスが網外非公開アドレス範囲にあることを検出すると前記外部パケットを廃棄するようになっており、前記送受信する IP パケットの当該 2 つの通信会社が合意した暗号、或いはデジタル署名を適用できるようになっている請求項 1 又は 2 に記載の統合情報通信システム。

【請求項 4】 前記変換表のレコードに仮想専用線を意味する要求識別を含まず、プライベートアドレス通信と非プライベートアドレス通信のみを行うようになっ

ている請求項 1 乃至 3 に記載の統合情報通信システム。

【発明の詳細な説明】

【0001】

【発明の属する分野】

本発明は、パソコン、LAN(Local Area Network)、電話（携帯電話やPHSを含む）、FAX(Facsimile)、CATV(Cable Television)、インターネット等の情報通信機器若しくは情報通信システムを専用線だけでなく、ISDN(Integrated Services Digital Network)、FR(Frame Memory)、ATM(Asynchronous Transfer Mode)、IPX(Integrated Packet Exchange)、衛星、無線、公衆回線を介して統合的に接続した統合情報通信システムに関する。ここでは、情報通信機器は、他と識別するための（情報通信用）アドレスを付与されて通信する。本発明は、特にコネクションレス型ネットワーク（例えばRFC791, RFC1883のIP(Internet Protocol) 技術)をベースとしたデータ転送サービスを統合して、一元的なアドレス体系の採用で情報通信全体の経済性を高め、セキュリティを確保して接続端末又はシステム間で相互通信できるようにした統合情報通信システムに関する。

【0002】

【従来の技術】

カプセル化技術を適用した統合情報通信システムとして、本出願人による特開平11-88438号公報に開示されたものがあり、本発明に関連する範囲を以下に説明する。

【0003】

即ち、統合情報通信システムは図16に示すように大きく内部と外部に分かれており、統合情報通信システムの内部では多数の中継装置がIP通信回線で結ばれており、統合情報通信システムの周辺部には複数のアクセス制御装置(AC)が設けられている。企業の多くのLANは、ユーザ通信回線を経てアクセス制御装置に接続される。この統合情報通信システムは、例えば1) IETF規定のプライベートIPアドレスを用いる“企業内通信”、2) プライベートIPアドレスを用いない“企業間通信”、3) 2つの端末を仮想的にIP通信回線により常時接

続したように見せる“仮想専用線”サービスの3通りを実現している。

【0004】

統合情報通信システムの外部と内部ではIPアドレスを使い分けており、統合情報通信システムの外部／内部で用いるIPアドレスを“外部／内部アドレス”と称している。統合情報通信システムの外部のIPパケットを“外部パケット”、統合情報通信システムの内部のIPパケットを“内部パケット”と称している。LANから送出された外部パケットは、ユーザ通信回線を経てアクセス制御装置に入力され、ユーザ通信回線の論理端子に付与されている内部アドレスを含むIPヘッダを付与されて内部パケットに変換され（カプセル化、図17参照）、統合情報通信システム内部を転送されて他のアクセス制御装置に到達し、ここで統合情報通信システム内部のIPヘッダを除かれて（逆カプセル化）、他のユーザ通信回線を経て通信相手先のLAN内部の端末に向けて送出される。

【0005】

ユーザ通信回線は図18に示すように、ユーザ物理通信回線91とユーザ論理通信回線92-1、92-2とに分けられ、ユーザ論理通信回線92-1とアクセス制御装置90の論理的な接点（ユーザ論理通信回線の終端）を論理端子（93-1、93-2）といい、論理端子を識別するためにIP網の内部アドレスを付与している。図18の例ではユーザ物理通信回線91はユーザ論理通信回線92-1及び92-2を含み、ユーザ論理通信回線92-1の終端（アクセス制御装置90との接点）としての論理端子93-1に内部アドレス“U”が付与され、ユーザ論理通信回線92-2の終端の論理端子93-2に内部アドレス“X”が付与されている。94-1乃至94-3はユーザ論理通信回線92-1、92-2に接続される端末である。物理通信回線を複数の論理通信回線に分けることは、例えばフレームリレー（のDLCI）やATM（のVPIやVCI）において実現されている。

【0006】

そして、特開平11-88438号の実施例15に「企業間通信の非カプセル化」の技法が開示されている。即ち、仮想専用線と企業内通信とでは、アクセス制御装置において外部パケットをカプセル化して内部パケットとし、統合情報通

信システム内を転送した後に、他のアクセス制御装置において逆カプセル化して外部パケットを復元し、ユーザ通信回線を経由して通信相手先に送達する技法が開示されている。企業間通信はカプセル化せずに、外部パケットをそのまま内部パケットとみなして統合情報通信システム内を転送し、（受信側の）他のアクセス制御装置からユーザ通信回線を経由して通信相手先端末に送達するようになっている。

【0007】

【発明が解決しようとする課題】

しかしながら、上述した従来の統合情報通信システムの内部には統合情報通信システムを運用管理するため各種網内サーバがあり、それぞれIPアドレスを有している。カプセル化しないアドレス範囲が存在する場合、IP網の外部から運用管理サーバへ大量のIPパケットが送信され、運用管理サーバの秘密データ読出し等などの不正アタックを受ける危険性が高くなる。

【0008】

本発明は上述のような事情よりなされたものであり、本発明の目的は、統合情報通信システムの外部から内部の運用管理サーバや中継装置へ向けて送出されてくるIPパケットを検出し、統合情報通信システム内部に侵入しないようにすることにより、統合情報通信システム内の運用管理サーバや中継装置が不正アタックを受ける機会を減らし、また、通信会社管理網内部と通信会社間通信に用いるIPパケットのアドレスを区分し、更に通信会社網の秘密保持を守るために付与しているアドレス付与規定に違反するIPパケットを検出し廃棄することにより安全性を向上させた統合情報通信システムを提供することにある。

【0009】

【課題を解決するための手段】

本発明は統合情報通信システムに関し、本発明の上記目的は、通信会社管理網を含む統合情報通信システムであり、前記通信会社管理網はアクセス制御装置、中継装置及びサーバを含み、前記アクセス制御装置、中継装置及びサーバは相互にIP通信回線で接続されており、前記通信会社管理網は境界中継装置を経て前記IP通信回線により接続されており、前記統合情報通信システムの外部の端末

はユーザ通信回線を経由して前記アクセス制御装置に接続され、前記ユーザ通信回線の終端の論理端子を識別するために、前記論理端子に内部アドレスが付与されると共に、前記アクセス制御装置は変換表を含み、前記変換表の要求識別が仮想専用線を意味する場合、外部パケットが入力した論理端子の識別情報が定まれば、送信側のアクセス制御装置が生成する内部パケットのヘッダに格納する内部宛先アドレスが一意に定まるように前記変換表のレコードとして登録されており、前記要求識別がプライベートアドレス通信を意味する場合、前記外部パケットが入力した論理端子の識別情報、外部ソースアドレス及び外部宛先アドレスの組が定まれば、前記送信側のアクセス制御装置が生成する内部パケットのヘッダに格納する内部宛先アドレスが一意に定まるように前記変換表のレコードとして登録されており、同一の論理端子識別情報に対して、前記外部宛先アドレス及び前記ヘッダ部に格納する内部宛先アドレスの組が共にレコード毎に異なり、同一論理端子から入力する外部パケット内の外部宛先アドレスを変更することにより前記外部パケットの到達先を変更できるようになっており、前記要求識別が非プライベートアドレス通信を意味する場合、前記論理端子識別情報及び外部ソースアドレスの組が前記変換表のレコードとして登録されており、当該登録は前記外部ソースアドレスを有する端末からの送信許可を意味し、前記外部パケットが前記端末から前記ユーザ通信回線に送信され、前記外部パケットが入力した論理端子の識別情報を含む前記変換表のレコードに、前記要求識別が仮想専用線と登録されていることが検出され、前記変換表から取得した論理端子識別情報及び内部宛先アドレスを用いて前記外部パケットから前記内部パケットに変換され、前記内部パケットは前記統合情報通信システム内部の前記IP通信回線及び中継装置を経由して転送され、受信側のアクセス制御装置の論理端子を経て他のユーザ通信回線を転送されて他の端末に到達するようになっており、前記アクセス制御装置内のパケットフィルタは、外部パケット内の宛先アドレスが網外非公開アドレスであることを検出すると、前記外部パケットを廃棄するようにすることによって達成される。

【 0 0 1 0 】

また、本発明の上記目的は、通信会社管理網を含む統合情報通信システムであ

り前記通信会社管理網はアクセス制御装置、中継装置及びサーバを含み、前記アクセス制御装置、中継装置及びサーバは相互に I P 通信回線で接続されており、前記通信会社管理網は境界中継装置を経て前記 I P 通信回線により接続されており、前記統合情報通信システムの外部の端末はユーザ通信回線を経由して前記アクセス制御装置に接続され、前記ユーザ通信回線の終端の論理端子を識別するために、前記論理端子に内部アドレスが付与されると共に、前記アクセス制御装置は変換表を含み、前記変換表の要求識別が仮想専用線を意味する場合、外部パケットが入力した論理端子の識別情報が定まれば、送信側のアクセス制御装置が生成する内部パケットのヘッダに格納する内部宛先アドレスが一意に定まるように前記変換表のレコードとして登録されており、前記要求識別がプライベートアドレス通信を意味する場合、外部パケットが入力した論理端子の識別情報、外部ソースアドレス及び外部宛先アドレスの組が定まれば、前記送信側のアクセス制御装置が生成する内部パケットのヘッダに格納する内部宛先アドレスが一意に定まるように前記変換表のレコードとして登録されており、同一の論理端子識別情報に対して、前記外部宛先アドレス及び前記ヘッダ部に格納する内部宛先アドレスの組が共にレコード毎に異なり、同一論理端子から入力する外部パケット内の外部宛先アドレスを変更することにより前記外部パケットの到達先を変更できるようになっており、前記要求識別がプライベートアドレス通信と登録されていることが見出されたとき、前記外部パケット内の外部ソースアドレス及び外部宛先アドレスが共に前記変換表のレコードに登録されていることが検出されたとき、前記変換表から取得した論理端子識別情報及び内部宛先アドレスを用いて前記外部パケットから前記内部パケットに変換され、前記要求識別が非プライベートアドレス通信と登録されていることが検出されたとき、前記外部パケット内の外部ソースアドレスが前記変換表のレコードに登録されていれば、前記外部ソースアドレスを有する端末の送信許可を確認できたので、前記外部パケットをそのまま前記内部パケットとし、前記内部パケットは前記統合情報通信システム内部の I P 通信回線と中継装置を経由して転送され、受信側のアクセス制御装置の論理端子を経て他のユーザ通信回線を転送され、他の端末に到達するようになっており、前記アクセス制御装置内のパケットフィルタは、前記外部パケット内の宛先アド

レスが網外非公開アドレスであることを検出すると、この外部パケットを廃棄するようにすることによって達成される。

【0011】

前記通信会社管理網間の前記IPパケットの送受信は通信会社間に共通のアドレスを用い、境界中継装置のパケットフィルタは、前記外部パケット内の宛先アドレスが網外非公開アドレス範囲にあることを検出すると前記外部パケットを廃棄するようになっており、前記送受信するIPパケットの当該2つの通信会社が合意した暗号、或いはデジタル署名を適用できるようにすることによって、より効果的に達成される。

【0012】

【発明の実施の形態】

本発明では、統合情報通信システム内の通信会社の運用管理用サーバや中継装置に付与するアドレスは、統合情報通信システムの外部に対して“網外非公開アドレス”として区分し、アクセス制御装置内にパケットフィルタを設置し、更に通信会社管理網間の通信は境界中継装置を経由し、境界中継装置内にパケットフィルタを設置する。

【0013】

アクセス制御装置内のパケットフィルタは、統合情報通信システムの外部から内部に入ってくる外部パケット内の宛先アドレスが、網外非公開アドレス範囲にあるか否かを調べ、網外非公開アドレス範囲にある場合は外部パケットを廃棄する。また、境界中継装置内のパケットフィルタは、通信会社管理網の間を送受信されるパケット内の宛先アドレスが通信会社内部アドレス範囲にあると検出された場合、パケットを廃棄する。

【0014】

本発明に基づくIPアドレスの第1の付与ルールを、図1を参照して説明する。統合情報通信システムの外部では、“プライベートアドレス”は“プライベートアドレス通信”に用い、“非プライベートアドレス”は“非プライベートアドレス通信”に用いる。ここで、プライベートアドレスは例えばRFC規定のアドレス区分を採用し、アドレス範囲の“10.0.0.0”～“10.255.255.255”、“172.16

“.0.0” ～ “172.16.255.255”、 “192.168.0.0” ～ “192.168.255.255” をプライベートアドレス範囲とし、他の全てのアドレス範囲を非プライベートアドレス範囲として I P パケット通信を行う方法である。

【 0 0 1 5 】

一方、統合情報通信システム内部では図 1 に示すように、非プライベートアドレスはそのまま網外公開アドレスとして位置付け、非プライベートアドレス通信に使用する。統合情報通信システムの内部のプライベートアドレス範囲は、“カプセル用アドレス”として内部パケットのヘッダ内部に設定するアドレスとして、及び“通信会社内部アドレス”として、通信会社のサーバや中継装置に付与するアドレスとして用いる。前述したように、統合情報通信システム内部のアドレスはユーザ通信回線の終端の論理端子に付与する。アドレスの第 1 の付与ルールは、プライベートアドレスの利用総数が少ないときは実用的であるが、プライベートアドレスの利用総数が多くなると、カプセル用のアドレスが不足する。

【 0 0 1 6 】

第 1 のルールの欠点を補うのが I P アドレスの第 2 の付与ルールであり、図 2 を参照して説明する。第 2 の規定においては、プライベートアドレス範囲の一部を“使用禁止アドレス”範囲とする方法である。この使用禁止アドレス範囲は、統合情報通信システムの内部において一部はカプセル用アドレス又は通信会社内部アドレスとする。

【 0 0 1 7 】

第 2 の付与ルールによるアドレス付与の例として、アドレス範囲の “.0.0.0.0” ～ “.255.255.255.255”、 “.172.16.0.0” ～ “.172.16.255.255”、 “.192.168.0.0” ～ “.192.168.255.255” をプライベートアドレス範囲とする。使用禁止アドレス範囲を、例えば “.240.0.0.0” ～ “.240.255.255.255” とする。

【 0 0 1 8 】

第 3 のルールは第 2 のルールの一部変更であり、使用禁止アドレス範囲は通信会社内部アドレスと通信会社間共通アドレスとに分けて用いる。なお、第 1 及び第 2 のルールは以下で説明する実施例 1 において、第 3 のルールは実施例 2 において採用している。残りのアドレス範囲を非プライベートアドレス範囲とする。

【 0 0 1 9 】

1. 実施例 1 :

図 3 の構成図を参照して説明する。統合情報通信システム 1 は内部にアクセス制御装置 2 - 1 乃至 2 - 4 を含むと共に、中継装置 3 - 1 乃至 3 - 4 を含み、LAN 0 1 は IP アドレス “p” である端末 7 - 1 を含み、LAN 0 2 は IP アドレス “q” である端末 7 - 2 を含み、LAN 0 3 は IP アドレス “a”、“b”、“c”、“d” である端末 8 - 1 乃至 8 - 4 を含み、LAN 0 4 は IP アドレス “e”、“k” である端末 9 - 1, 9 - 2 を含み、LAN 0 5 は IP アドレス “f”、“m” である端末 1 0 - 1, 1 0 - 2 を含み、端末 6 - 1 の IP アドレスは “g” であり、端末 6 - 2 の IP アドレスは “h” である。

【 0 0 2 0 】

また、統合情報通信システム 1 の外部で使用するアドレスを外部アドレス、内部で使用するアドレスを内部アドレスといい、IP パケットのソース側（送信側）のアドレスをそれぞれ統合情報通信システム 1 の外部及び内部に対応させて、それぞれ “外部ソースアドレス” 及び “内部ソースアドレス” で表わし、IP パケットの宛先側（受信側）のアドレスを統合情報通信システム 1 の外部及び内部に対応させて、それぞれ “外部宛先アドレス” 及び “内部宛先アドレス” でわす。

【 0 0 2 1 】

通信回線 1 1 - 1 とアクセス制御装置 2 - 1 との接点の論理端子に内部アドレス “U” を付与してあり、通信回線 1 1 - 2 とアクセス制御装置 2 - 4 との接点の論理端子に内部アドレス “V” を付与してある。通信回線 1 1 - 3 とアクセス制御装置 2 - 1 との接点の論理端子に内部アドレス “X” を付与してあり、通信回線 1 1 - 4 とアクセス制御装置 2 - 4 との接点の論理端子に内部アドレス “Y” を付与してあり、通信回線 1 1 - 5 とアクセス制御装置 2 - 3 との接点の論理端子に内部アドレス “Z” を付与してある。また、端末 6 - 1 から通信回線 1 2 - 1 を経てアクセス制御装置 2 - 2 に接続し、通信回線 1 2 - 1 の終端の論理端子に内部アドレス “P” を付与してあり、端末 6 - 2 から通信回線 1 2 - 2 を経

てアクセス制御装置 2-3 に接続し、通信回線 12-2 の終端の論理端子に内部アドレス “W” を付与してある。

【 0 0 2 2 】

アクセス制御装置 2-1 はパケットフィルタ 13 及び変換表 17 を含み、アクセス制御装置 2-2 はパケットフィルタ 14 及び変換表 18 を含み、アクセス制御装置 2-3 はパケットフィルタ 15 及び変換表 19 を含み、アクセス制御装置 2-4 はパケットフィルタ 16 及び変換表 20 を含んでいる。中継装置 3-1 乃至 3-4、網代表サーバ 4-1、ユーザサービスサーバ 4-2、資源管理サーバ 4-3、表管理サーバ 4-4 及び 4-5 はそれぞれ統合情報通信システム 1 の内部アドレスを付与されており、更に IP パケット転送機能を有する IP 通信回線を経由して直接的に、あるいは中継装置を経由して間接的に接続されており、相互に IP パケットを送受信し情報交換できる IP 通信手段を有する。

【 0 0 2 3 】

<<準備>>

LAN 01 の利用責任者 30-1 及び LAN 02 の利用責任者 30-2 は、LAN 01 及び LAN 02 の間に統合情報通信システム 1 を経由して仮想専用線を設定することに合意し、統合情報通信システム 1 のサービス受付者 31 に IP 通信回線の登録を申込むと、サービス受付者 31 はユーザサービスサーバ 4-2 を操作し、ユーザサービスサーバ 4-2 は代表サーバ 4-1 及びリソース管理サーバ 4-3 と IP 通信手段を用いて情報交換し、更に表管理サーバ 4-4 及び 4-5 に依頼して、アクセス制御装置 2-1 内部の変換表 17 とアクセス制御装置 2-4 内部の変換表 20 に、以下に述べる手順によりアドレスや優先度などを設定する。

【 0 0 2 4 】

即ち、表管理サーバ 4-4 は、アクセス制御装置 2-1 内の図 4 に示す変換表 17 の第 1 レコード（変換表の 1 行目）に、内部ソースアドレスとして “U” を、内部宛先アドレスとして “V” を、要求識別として仮想専用線を意味する “3” を、優先度として “4” を、課金識別子として “Fa01” をそれぞれ設定（登録）する。同様に、表管理サーバ 4-5 は、アクセス制御装置 2-4 内の図 7 に示

す変換表 2 0 の第 1 レコードに、内部ソースアドレス “V” を、内部宛先アドレス “U” を、要求識別として仮想専用線を意味する “3” を、優先度として “4” を、課金識別子として “Fc01” を設定する。

【 0 0 2 5 】

上述と同様な手順により、表管理サーバ 4 - 4 はユーザサービスサーバ 4 - 2 から I P 通信手段を用いて依頼され、アクセス制御装置 2 - 1 内の変換表 1 7 の第 2 レコードに、内部ソースアドレスとして “X” を、外部ソースアドレスとして “a” を、外部宛先アドレスとして “k” を、内部宛先アドレスとして “Y” を、要求識別としてプライベートアドレス通信を意味する “1” を、優先度として “2” を、課金識別子として “Fa02” をそれぞれ設定し、更に変換表 1 7 の第 3 レコードに、内部ソースアドレスとして “X” を、外部ソースアドレスとして “b” を、外部宛先アドレスとして “m” を、内部宛先アドレスとして “Z” を、要求識別としてプライベートアドレス通信を意味する “1” を、優先度として “2” を、課金識別子として “Fa03” をそれぞれ設定する。更に、変換表 1 7 の第 4 レコードに、内部ソースアドレスとして “X” を、外部ソースアドレスとして “c” を、要求識別として非プライベートアドレス通信を意味する “2” を、優先度として “0” を、課金識別子として “Fa04” をそれぞれ設定し、変換表 1 7 の第 5 レコードに、内部ソースアドレスとして “X” を、外部ソースアドレスとして “d” を、要求識別として非プライベートアドレス通信を意味する “2” を、優先度として “0” を、課金識別子として “Fa05” をそれぞれ設定する。

【 0 0 2 6 】

端末 6 - 1 の利用者が端末 6 - 1 の登録をサービス受付者 3 1 に申込み、ユーザサービスサーバ 4 - 2 から I P 通信手段を用いて依頼された表管理サーバ 4 - 4 は、アクセス制御装置 2 - 2 内の図 5 に示す変換表 1 8 の第 1 レコードに、内部ソースアドレスとして “P” を、外部ソースアドレスとして “g” を、要求識別として非プライベートアドレス通信を意味する “2” を、優先度として “0” を、課金識別子として “Fb01” をそれぞれ設定する。同様に、端末 6 - 2 の利用者が、端末 6 - 2 の登録をサービス受付者 3 1 に申込み、ユーザサービスサーバ 4 - 2 から I P 通信手段を用いて依頼された表管理サーバ 4 - 5 は、アクセス制

御装置 2 - 3 内の図 6 に示す変換表 1 9 の第 1 レコードに、内部ソースアドレスとして“W”を、外部ソースアドレスとして“h”を、要求識別として“2”を、優先度として“0”を、課金識別子として“Fd01”をそれぞれ設定する。

【 0 0 2 7 】

更に、LAN05の利用責任者の依頼に基づき変換表 1 9 の第 2 レコードに、内部ソースアドレスとして“Z”を、外部ソースアドレスとして“m”を、外部宛先アドレスとして“b”を、内部宛先アドレスとして“X”を、要求識別として“1”を、優先度として“2”を、課金識別子として“Fd02”をそれぞれ設定し、変換表 1 9 の第 3 レコードに、内部ソースアドレスとして“Z”を、外部ソースアドレスとして“f”を、要求識別として“2”を、優先度として“0”を、課金識別子として“Fd03”をそれぞれ設定する。

【 0 0 2 8 】

同様に、LAN04の利用責任者の依頼に基づき、ユーザサービスサーバ 4 - 2 から IP 通信手段を用いて依頼された表管理サーバ 4 - 5 は、変換表 2 0 の第 2 レコードに、内部ソースアドレスとして“Y”を、外部ソースアドレスとして“k”を、外部宛先アドレスとして“a”を、内部宛先アドレスとして“X”を、要求識別として“1”を、優先度として“2”を、課金識別子として“Fc02”をそれぞれ設定し、変換表 2 0 の第 3 レコードに、内部ソースアドレスとして“Y”を、外部ソースアドレスとして“e”を、要求識別として“2”を、優先度として“0”を、課金識別子として“Fc03”をそれぞれ設定する。

【 0 0 2 9 】

<< 仮想専用線の利用 >>

仮想専用線による IP パケット転送の流れを、図 8 を参照して説明する。

【 0 0 3 0 】

LAN01内の端末 7 - 1 から、外部ソースアドレス“p”及び外部宛先アドレス“q”である外部パケット 4 0 がユーザ通信回線 1 1 - 1 に送出され、アクセス制御装置 2 - 1 は外部パケット 4 0 を受信し（図 8 のステップ S01）、外部パケット 4 0 はユーザ通信回線 1 1 - 1 の終端の論理端子から入力し、論理端子に付与された内部アドレス“U”を有する変換表 1 7 のレコードを検索し（ステップ S02

）、内部アドレス“U”を含むレコードが変換表17に未登録ならば外部パケット40を廃棄する（ステップS03）。本ケースでは登録してあるので、上述で検索した変換表17の第1レコードの要求識別の値を調べ（ステップS04）、本ケースでは仮想専用線を意味する値“3”であるので、第1レコードの内部宛先アドレス“V”を取得し、上述で取得した内部ソースアドレス“U”と内部宛先アドレス“V”とを用いてカプセル化を行って内部パケットを生成する（ステップS05）。次に第1レコードの優先度“4”を、上述で生成した内部パケット内ヘッダの優先度フィールド（例えばRFC791規定のTOSフィールド）に格納し（ステップS06）、網内へ転送する（ステップS07）。課金識別子“Fa01”が指す領域には、例えばアクセス制御装置2-1が生成した内部パケットの数の積算値やパケット長など課金に関する情報を記録する。

【0031】

上述により生成された内部パケット41は、網内のパケット転送ルールに従い中継装置3-1、3-4を経由してアクセス制御装置2-4に到達される。中継装置3-1及び3-4は中継表を含み、パケットの転送先を決定している。次に、アクセス制御装置2-4は内部パケット41を受信すると（図9のステップS21）、内部パケット41内の内部宛先アドレス“V”が、変換表20の内部ソースアドレスとして含むレコードを検索し（ステップS22）、当該レコードが変換表20に存在しなければ内部パケット41を廃棄する（ステップS23）。本ケースでは変換表20の第1レコードの内部ソースアドレスが“V”であるので、上述で検出した第1レコードの要求識別の値を調べる（ステップS24）。本ケースでは仮想専用線を意味する値“3”であるので、逆カプセル化されて外部パケット42が復元され（ステップS25）、前記復元された外部パケットが統合情報通信システムの外部に送出され（ステップS26）、ユーザ通信回線11-2を経てLAN02内部の端末7-2に到達する。

【0032】

上述で説明した仮想専用線による通信に用いるアドレス範囲は第1のルール及び第2のルールのいずれにも限定されるものではなく、任意のアドレス範囲が可能である。

【 0 0 3 3 】

<<プライベートアドレス通信>>

LAN 0 3 内の外部ソースアドレスが “a” である端末 8 - 1 から、LAN 0 4 内の外部アドレス “k” である端末 9 - 2 へ向けて外部パケット 4 3 が送出されると、アクセス制御装置 2 - 1 は外部パケット 4 3 を受信し（図 8 のステップ S01）、ユーザ通信回線 1 1 - 3 の論理端子に付与された内部アドレス “X” を、内部ソースアドレスの項目として含む変換表 1 7 のレコードを検索し（ステップ S02）、仮想専用線でないかを調べる（ステップ S04）。本ケースでは変換表 1 7 の第 2 レコードとして登録してあるので、第 2 レコードの要求識別の値を調べる（ステップ S08）。本ケースではプライベートアドレス通信を意味する値 “1” であるので、前記入力した論理端子に付与された内部アドレス “X”、外部パケットのヘッダ内の外部ソースアドレス “a”、外部宛先アドレス “k” の組が、変換表 1 7 の第 2 レコードに含まれる内部ソースアドレス “X”、外部ソースアドレス “a”、外部宛先アドレス “k” の組と一致するので、第 2 レコードの内部宛先アドレス “Y” を取得して、内部ソースアドレス “X” 及び内部宛先アドレス “Y” を用いてカプセル化を行って内部パケット 4 4 を生成し（ステップ S09）、前記 2 行目のレコードの優先度 “2” をカプセルの優先度フィールドに格納し（ステップ S06）、網内へ転送する（ステップ S07）。

【 0 0 3 4 】

上述により生成された内部パケット 4 4 は、網内の IP パケットルールに従い中継装置 3 - 1、3 - 4 を経由してアクセス制御装置 2 - 4 に到達し、アクセス制御装置 2 - 4 は内部パケット 4 4 を受信すると（図 9 のステップ S 2 1）、内部パケット 4 4 内の内部宛先アドレス “Y” を、変換表 2 0 の内部ソースアドレスとして含むレコードを検索し（ステップ S22）、当該レコードが変換表 2 0 に存在しなければ内部パケット 4 4 を廃棄する（ステップ S23）。本ケースでは変換表 2 0 の第 2 レコードの内部ソースアドレスが “Y” であるので、上述で検出した第 2 レコードの要求識別の値を調べる（ステップ S24）。本ケースではプライベートアドレス通信を意味する値 “1” であるので（ステップ S27）、逆カプセル化され（ステップ S28）て外部パケット 4 5 が復元され、統合情報通信システ

ムの外部に送出され（ステップS26）、外部パケット45はユーザ通信回線11-4を経て、LAN04内のIPアドレス“k”である端末9-2に到達する。

【0035】

なお、前記ステップS27は、外部宛先アドレス“k”を有するレコードが変換表20の第2のレコードとして検出できるケースである。もし、外部宛先アドレス“k”を有するレコードが、変換表20のレコードとして検出できない場合は、前記受信した内部パケットを前記のステップS27において、廃棄することもできる。

【0036】

LAN03の内の外部ソースアドレス“b”である端末8-2から、LAN05内部の外部宛先アドレスが“m”である端末10-2への通信も同様に可能である。本ケースにおいては、アクセス制御装置2-1内の変換表17の第3のレコードと、アクセス制御装置2-3内の変換表19の第2のレコードとが使用される。従って、ユーザ通信回線11-3から入力したIPパケットの外部宛先アドレスを変えることにより、外部パケットの到達先を変更することができる。

【0037】

<<非プライベートアドレス通信>>

LAN03内の外部ソースアドレスが“c”である端末8-3から、LAN04内の外部アドレスが“e”である端末9-1へ向けて外部パケット50が送出されると、アクセス制御装置2-1は、ユーザ通信回線11-3の論理端子を経由して外部パケット50を受信し（図8のステップS01）、外部パケット50が入力した論理端子に付与された内部アドレス“X”を、内部ソースアドレスの項目として含む変換表17のレコードを検索し（ステップS02）、変換表17に該当するレコードが登録してなければ外部パケット50を廃棄する（ステップS03）。本ケースでは変換表17の第4レコードとして登録してあるので、当該第4レコードの要求識別の値を調べる（ステップS04、ステップS08）。本ケースでは非プライベートアドレス通信を意味する値が“2”であるので、アクセス制御装置2-1は、外部パケット50の外部ソースアドレスが網外非公開アドレスの範囲にあるか否かをパケットフィルタ13を用いて調べ（ステップS10）、網外非

公開アドレスである場合は外部パケット 5 0 を破棄し（ステップ S03）、網外公開アドレスである場合は、カプセル化を行わずに外部パケット 5 0 をそのまま内部パケットとし、第 4 レコードの優先度“0”をカプセルの優先度フィールドに格納し（ステップ S06）、網内へ転送する（ステップ S07）。

【 0 0 3 8 】

上述により生成された内部パケット 5 1 は、網内の IP パケットルールに従い中継装置 3 - 1, 3 - 4 を通過して転送され、アクセス制御装置 2 - 4 は内部パケット 5 1 を受信すると（図 9 のステップ S21）、内部パケット 5 1 内部の内部宛先アドレスを調べる。本ケースでは、内部宛先アドレス“e”を含む変換表 2 0 のレコードを検索し（ステップ S22）、内部アドレス“e”を含むレコードが変換表 2 0 に登録してなければ内部パケット 5 1 を廃棄する（ステップ S23）。本ケースでは第 3 レコードとして登録してあるので、当該第 3 レコードの要求識別の値を調べる（ステップ S24、S27）。本ケースでは非プライベートアドレス通信を意味する値“2”であるので、逆カプセル化を行わずに内部パケット 5 1 はそのまま外部パケット 5 2 となり、統合情報通信システムの外部に送出され（ステップ S26）、外部パケット 5 2 はユーザ通信回線 1 1 - 4 を経て、LAN 0 4 内の IP アドレス“e”である端末 9 - 1 に到達する。

【 0 0 3 9 】

LAN 0 3 内の外部ソースアドレスが“d”である端末 8 - 4 から、LAN 0 5 内部の外部宛先アドレス“f”である端末 1 0 - 1 への通信も同様に可能である。本ケースにおいては、アクセス制御装置 2 - 1 内の変換表 1 7 の第 5 のレコードと、アクセス制御装置 2 - 3 内の変換表 1 9 の第 3 レコードとが使用される。

【 0 0 4 0 】

a. パケットフィルタの位置：

前記の説明において、パケットフィルタの機能は非プライベートアドレス通信の判定における手順において実施している。なお、パケットフィルタの機能は、カプセル化の手順において、他の位置において実施しても良い。例えば図 1 0 に示すように、ステップ S51（外部パケット受信）の直後においてパケットフィルタの機能を実施してもよく、外部パケットから内部パケットに変換する過程であ

れば、パケットフィルタをどの場所においても良い。

【 0 0 4 1 】

b. 各種サーバ：

代表サーバ 4 - 1 は、ユーザサービスサーバ 4 - 2、リソース管理サーバ 4 - 3、表管理サーバ 4 - 4 乃至 4 - 5 などに、それぞれのサーバの運用開始などの指示を与え、あるいは運用状況などの個別報告をさせる。リソース管理サーバ 4 - 3 は、中継装置 3 - 1 乃至 3 - 4 やアクセス制御装置 2 - 1 乃至 2 - 4 などの動作状況や障害情報を把握する。

【 0 0 4 2 】

c. 仮想専用線を用いないとき：

本実施例において、仮想専用線を用いずにプライベートアドレス通信と非プライベートアドレス通信のみを実施することができる。このためには、変換表 1 7 乃至 2 0 において要求識別が仮想専用線を意味するレコードを削除し、例えば変換表 1 7 の第 1 レコード及び変換表 2 0 の第 1 レコードを削除し、更に図 8 に示す仮想専用線か否かを判定するステップ S04 を省略し、図 9 に示す仮想専用線か否かを判定するステップ S24 を省略する。

【 0 0 4 3 】

d. 他の情報安全性の向上方法：

各サーバは、内部パケットのソースアドレスが網外公開アドレス範囲にあることを検出すると、内部パケットの情報アクセスを拒否するようにすることにより、更に情報安全性を向上させることができる。また、統合情報通信システム内部のサーバは、外部パケットからその網外非公開アドレスを要求されても回答しないようにして、網内部の秘密アドレスが外部に漏出するのを予防することもできる。

【 0 0 4 4 】

2. 実施例 2：

本発明の第 2 実施例を、図 1 1 乃至図 1 4 を参照して説明する。本実施例における統合情報通信システム 5 7 は、通信会社 “A” の通信会社管理網 5 8 と、通

信会社“B”の通信会社管理網59と、境界中継装置61及び境界中継装置62を結ぶIP通信回線60とから構成されている。境界中継装置61内にパケットフィルタ63があり、境界中継装置62内にパケットフィルタ64がある。アクセス制御装置65-1乃至65-7、中継装置66-1、66-2、LAN67-1、LAN67-2である。

【0045】

先ず図14を参照して、IPアドレスの使い方を説明する。アドレス付与のルールは前述した第3のルールであり、禁止アドレス範囲は、通信会社管理網58及び通信会社管理網59の内部において、一部はカプセル用アドレス、一部は通信会社内部アドレス、他は通信会社間共通アドレスに付与して用いる。

【0046】

a. 通信会社内部アドレス：

通信会社“A”及び“B”は、共に通信会社内部アドレス範囲として“240.0.0.0”～“240.255.255.255”を用いる。

【0047】

b. 通信会社間共通アドレス：

通信会社“A”及び“B”共に通信会社間共通アドレスとして“241.0.0.0”～“241.255.255.255”を用いる。

【0048】

c. 外部パケットのカプセル化用のアドレス：

カプセル用アドレスとして“242.0.0.0”～“255.255.255.255”及びIETF規定のプライベートアドレス範囲、即ち“10.0.0.0”～“10.255.255.255”、“172.16.0.0”～“172.16.255.255”、“192.168.0.0”～“192.168.255.255”を用いる。

【0049】

d. 非プライベートアドレス通信用のアドレス：

上述した通信会社内部アドレス、通信会社間共通アドレス及びカプセルアドレスの全てを除いた範囲のアドレスを用いる。IP通信回線60内は、内部IPパケットや通信会社間において送受信するIPパケットが送受信される。

【 0 0 5 0 】

e. 境界中継装置のパケットフィルタ :

図 1 1 において、パケットフィルタ 6 3 や 6 4 は、他の通信会社管理網から I P パケットを受信すると (図 1 2 のステップ S30)、その宛先アドレスを調べ (ステップ S31)、この宛先アドレスが通信会社内部アドレス範囲、つまり “240.0.0.0~240.255.255.255” である場合は、この I P パケットを廃棄し (ステップ S32)、そうでない場合は受け入れる (ステップ S33)。

【 0 0 5 1 】

また、図 1 1 において、パケットフィルタ 6 3 及び 6 4 は、自社の通信会社管理網の内部から I P パケット送出要求を受取ると (図 1 3 のステップ S40)、その宛先アドレスを調べ (ステップ S41)、この宛先アドレスが通信会社内部アドレス範囲、つまり “240.0.0.0~240.255.255.255” である場合はこの I P パケットを廃棄し (ステップ S42)、そうでない場合は、当該 I P パケットを他の通信会社管理網へ送出する (ステップ S43)。

【 0 0 5 2 】

f. アドレス値の選定 :

上記アドレス範囲は数値例であり、他のアドレス範囲を選択しても良く、未割当アドレス範囲を設定しても良い。例えば 3 2 ビット長アドレスの場合、図 1 4 のアドレス区分において、I P 網の外部においてはプライベートアドレス通信範囲を “0.0.0.0” ~ “1.255.255.255”、禁止アドレス範囲を “2.0.0.0” ~ “2.255.255.255”、共通アドレス範囲を “3.0.0.0” ~ “3.255.255.255”、非プライベート通信アドレス範囲を “4.0.0.0” ~ “254.255.255.255”、未割当アドレス範囲を “255.0.0.0” ~ “255.255.255.255” とする。また、I P 網の内部においては網外非公開アドレスの範囲を “0.0.0.0” ~ “3.255.255.255”、網外公開アドレス範囲を “4.0.0.0” ~ “254.255.255.255”、未割当アドレス範囲を “255.0.0.0” ~ “255.255.255.255” とする。

【 0 0 5 3 】

ここで、未割当アドレス範囲はパケットの送受信実験などに用いることができる。R F C 1 8 8 3 規定の 1 2 8 ビット長アドレスの場合や、他のアドレス長の

場合であってもそれぞれ同様にアドレス範囲を定めることができる。

【 0 0 5 4 】

g. 通信会社の運用網が 3 以上のケース：

本実施例は通信会社管理網が 2 つのケースであるが、通信会社管理網が 3 以上の場合も、通信会社間の I P パケット送受信は通信会社間共通アドレスを用い、通信管理網内部では通信会社内部アドレスを用いる。通信会社 P と通信会社 Q との間で IP パケットを送受信する場合、その IP パケットのデータ（ペイロード）の部分は、通信会社 P と通信会社 Q が個別に合意して定めた暗号技術を適用して暗号文とし、或いはデジタル署名の技術を適用して、データとデータに関する電子署名を I P パケットのペイロードに格納することもできる。

【 0 0 5 5 】

h. 非プライベートアドレス通信の他の例：

非プライベートアドレス通信において、外部パケットをカプセル化して内部パケットを生成する方法を採用しても、境界中継装置のパケットフィルタを用いることができる。特開平 1 1 - 8 8 4 3 8 号公報に示される実施例 1 5 を除く他の実施例において、アドレス区分は図 1 5 に示すように、I P 網の外部においてはプライベートアドレス通信と非プライベートアドレス通信とに分け、I P 網の内部においては網外非公開アドレス範囲に分けられている。なお、I P 網の外部のアドレスと I P 網の内部とのアドレスは無関係に決められている。

【 0 0 5 6 】

1 つの通信会社管理網から他の通信会社管理網の間を通信回線により接続する中継装置において、図 1 2 及び図 1 3 に示すように通信会社内部アドレスを検出し、廃棄するためのパケットフィルタを機能させることができる。

【 0 0 5 7 】

【発明の効果】

上述したように、本発明によれば仮想専用線による通信やプライベートアドレス通信においては、アクセス制御装置において、外部パケットをカプセル化して内部パケットとして転送し、非プライベートアドレス通信においては、カプセル化せずに内部を転送する統合情報通信網において、アクセス制御装置と境界中継

•

出証特 2 0 0 1 - 3 0 4 7 8 8 2

る受信側のアクセス制御装置の動作例を示すフローチャートである。

【図 1 0】

外部パケットを受信して内部パケットを生成し、網内へ内部パケットを送出する送信側のアクセス制御装置の他の動作例を示すフローチャートである。

【図 1 1】

本発明の第 2 実施例の構成を示すブロック図である。

【図 1 2】

境界中継装置のアドレスフィルタの機能を説明するための図である。

【図 1 3】

境界中継装置のアドレスフィルタの機能を説明するための図である。

【図 1 4】

第 2 実施例のアドレス区分の例を示す図である。

【図 1 5】

第 2 実施例のアドレス区分の例を示す図である。

【図 1 6】

統合情報通信システムの概略構成を示すブロック図である。

【図 1 7】

カプセル化を説明するための図である。

【図 1 8】

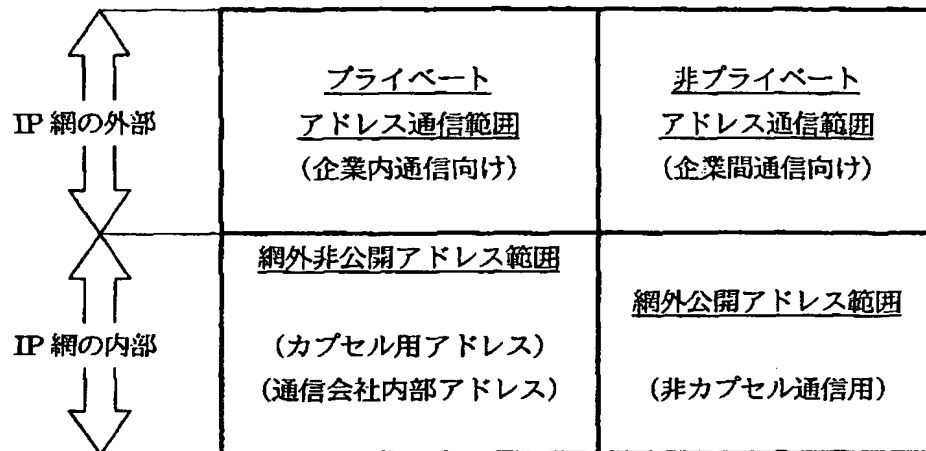
ユーザ通信回線を説明するための図である。

【符号の説明】

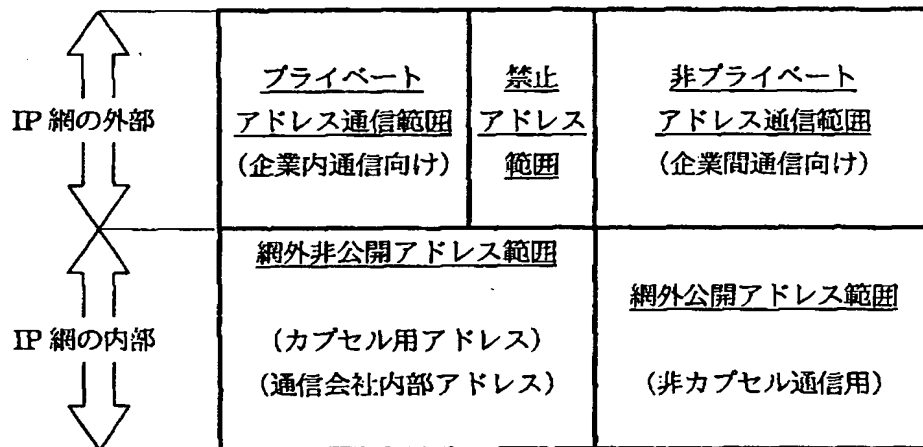
- 1 統合情報通信システム
- 2 - 1 ~ 2 - 4 アクセス制御装置
- 3 - 1 ~ 3 - 4 中継装置
- 4 - 2 ユーザサービスサーバ
- 4 - 3 資源管理サーバ
- 4 - 4, 4 - 5 表管理サーバ
- 3 1 サービス受付者

【書類名】 図面

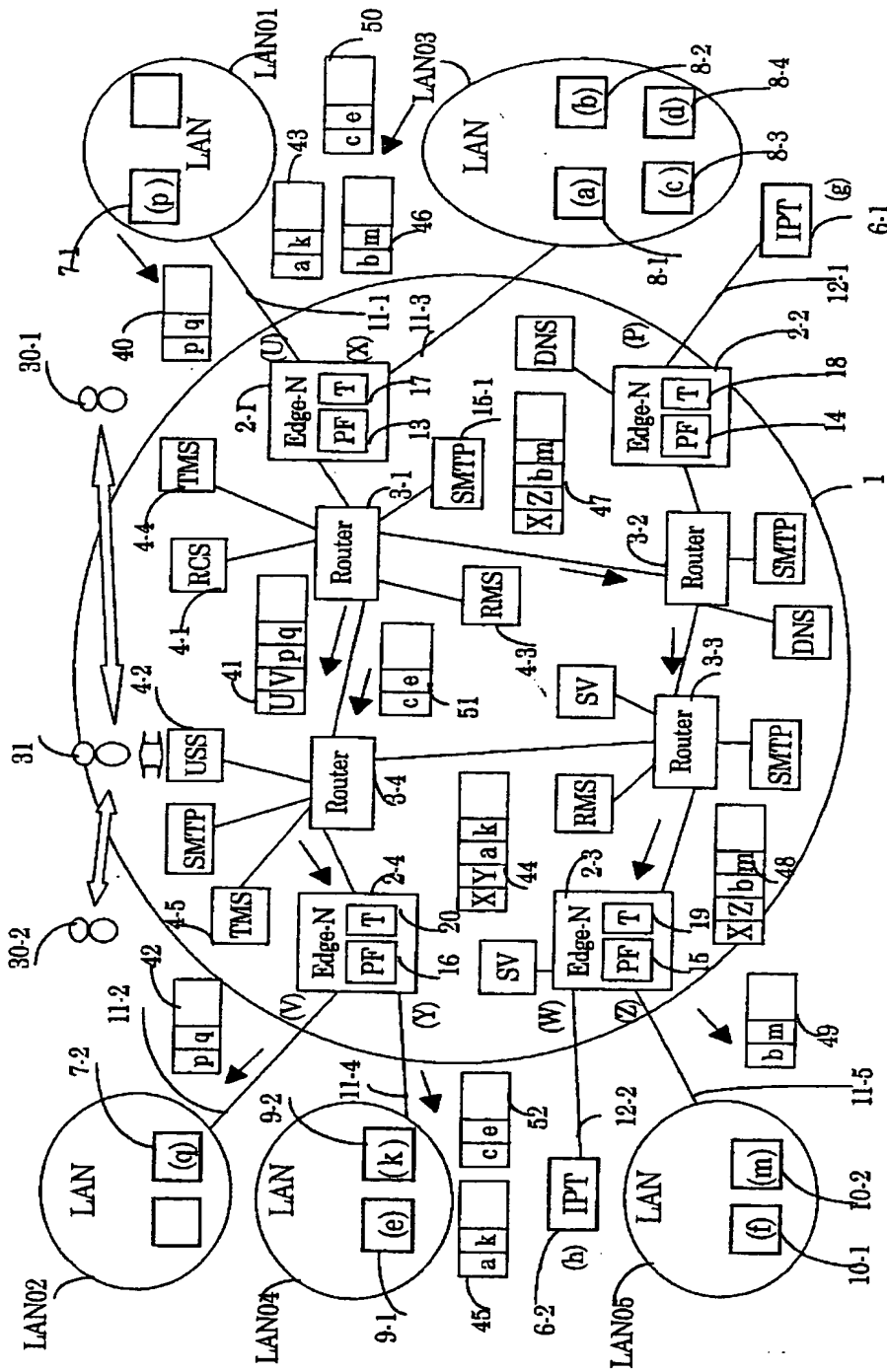
【図 1】



【図 2】



【図3】



【図 4】

17

内部ソース アドレス	外部ソース アドレス	外部宛先 アドレス	内部宛先 アドレス	要求 識別	優先度	課金 識別子
U	—	—	V	3	4	Fa01
X	a	k	Y	1	2	Fa02
X	b	m	Z	1	2	Fa03
X	c	—	—	2	0	Fa04
X	d	—	—	2	0	Fa05
..

【図 5】

18

内部ソース アドレス	外部ソース アドレス	外部宛先 アドレス	内部宛先 アドレス	要求 識別	優先度	課金 識別子
P	g	—	—	2	0	Fb01
..

【図 6】

19

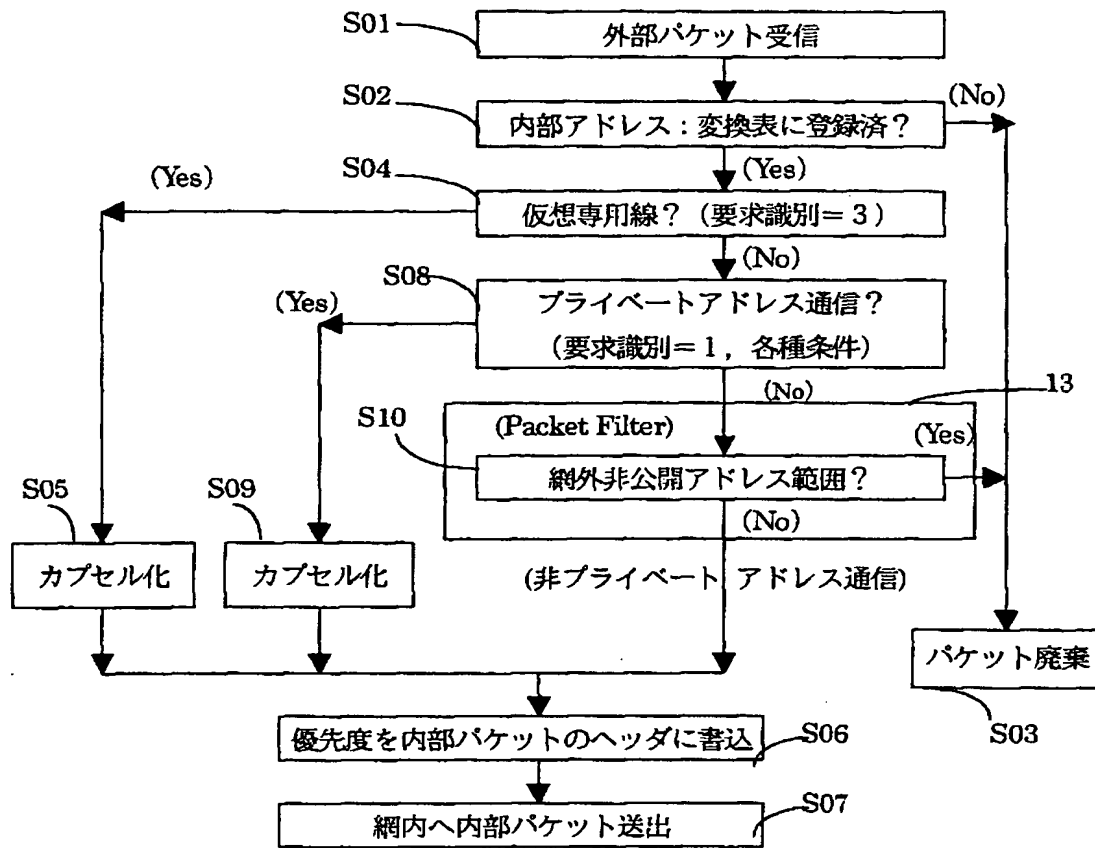
内部ソース アドレス	外部ソース アドレス	外部宛先 アドレス	内部宛先 アドレス	要求 識別	優先度	課金 識別子
W	h	—	—	2	0	Fd01
Z	m	b	X	1	2	Fd02
Z	f	—	—	2	0	Fd03
..

【図 7】

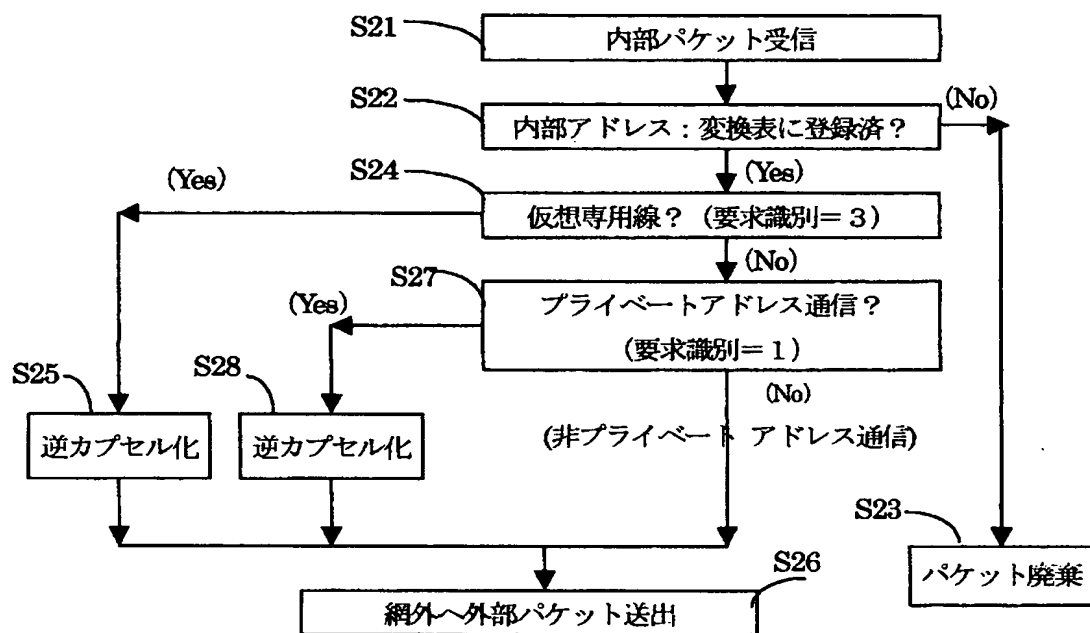
20

内部ソース アドレス	外部ソース アドレス	外部宛先 アドレス	内部宛先 アドレス	要求 識別	優先度	課金 識別子
V	—	—	U	3	4	Fc01
Y	k	a	X	1	2	Fc02
Y	e	—	—	2	0	Fc03
..

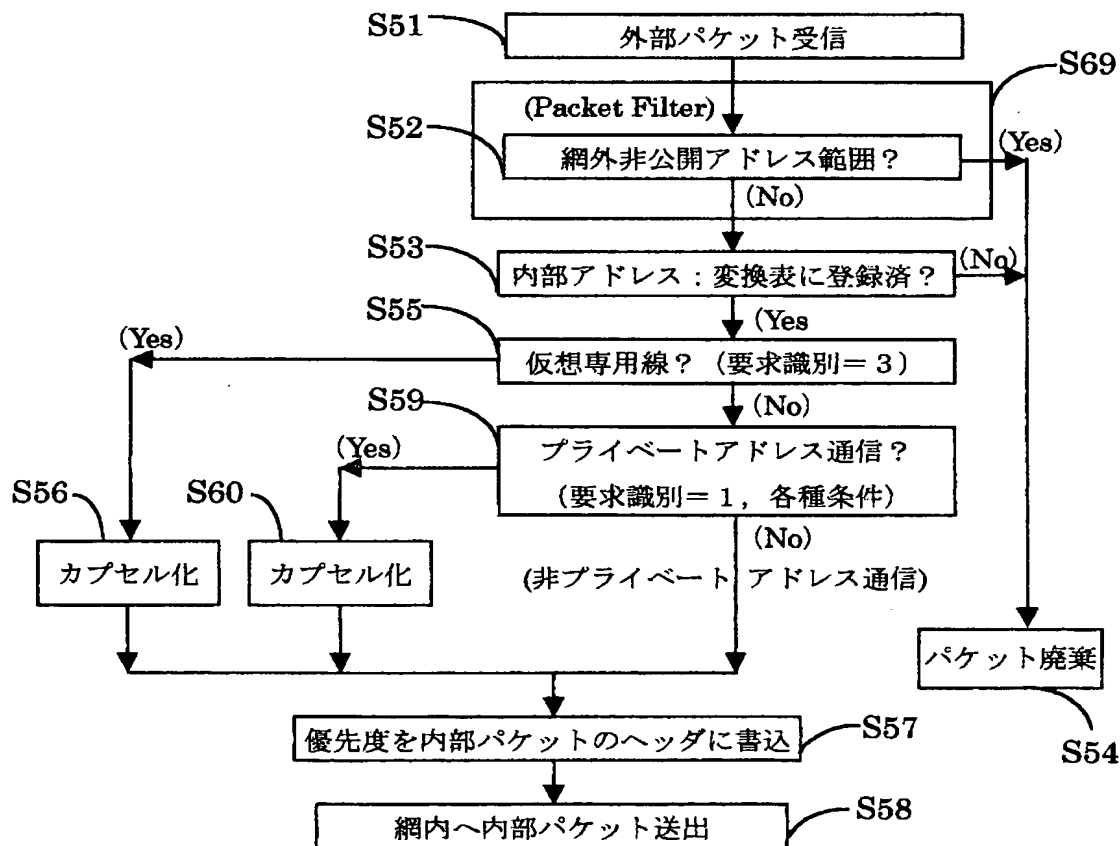
【図 8】



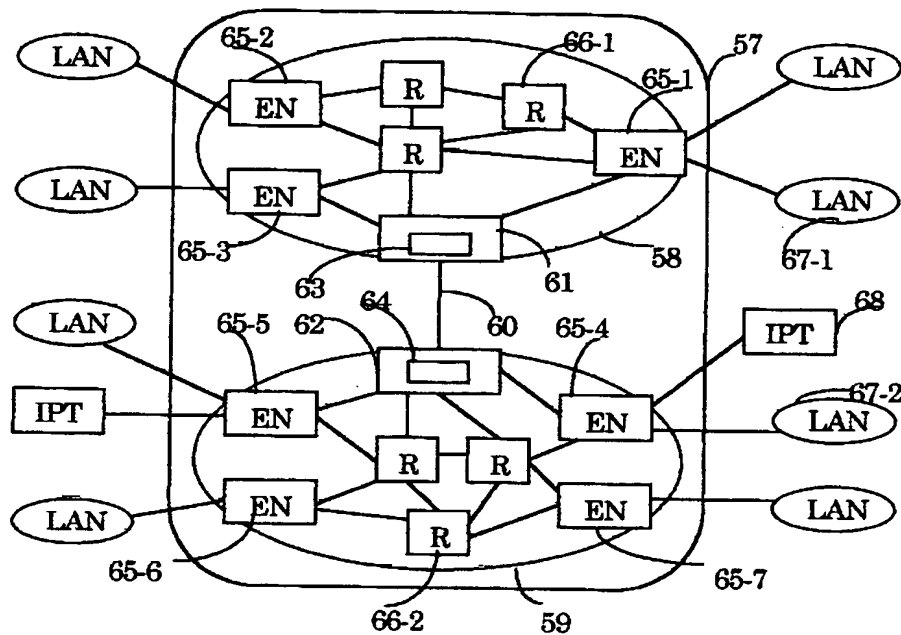
【図 9】



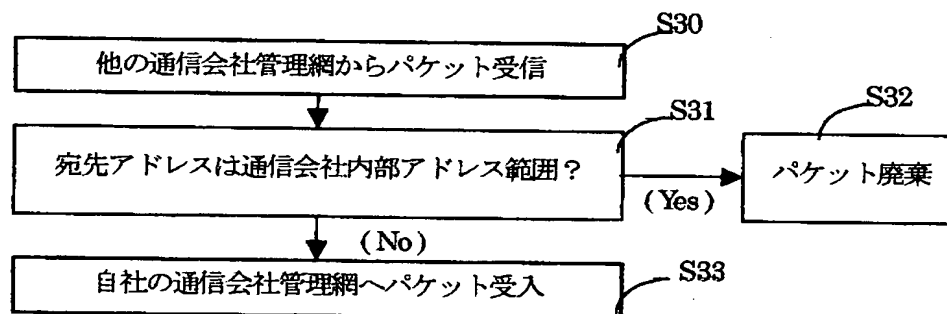
【図 10】



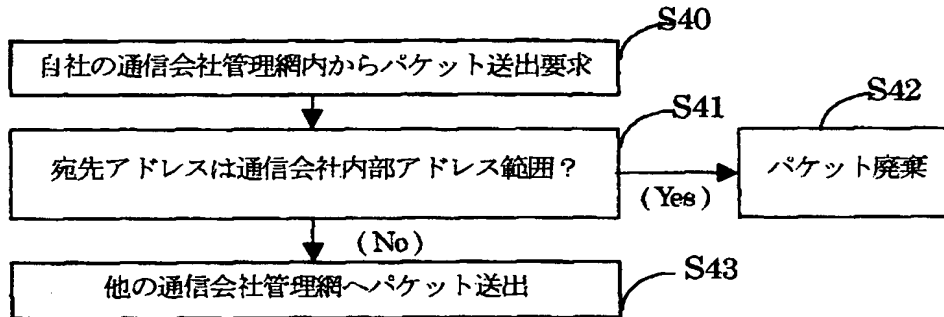
【図 1 1】



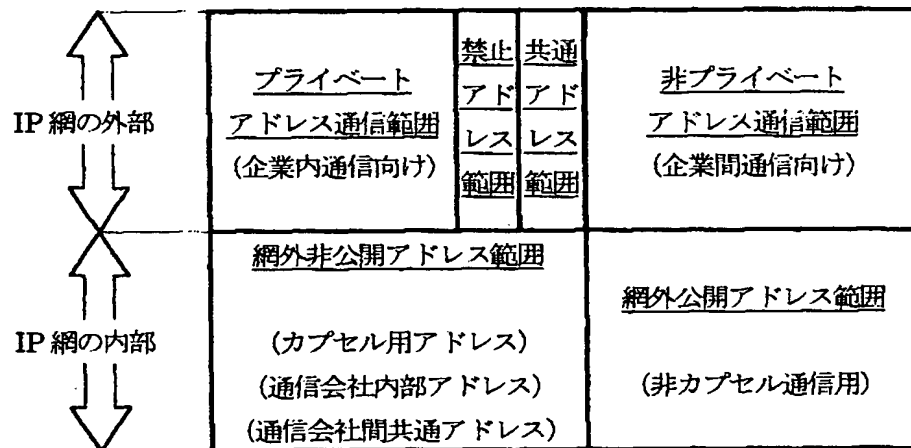
【図 1 2】



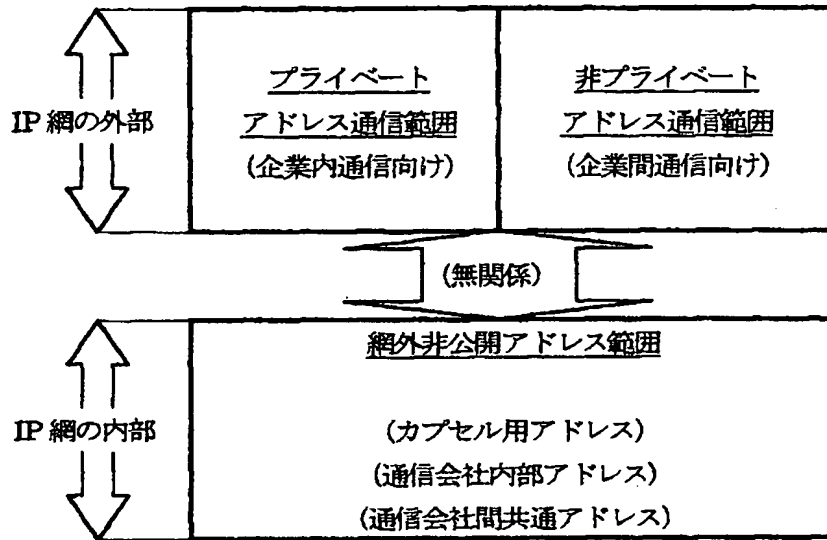
【図 1 3】



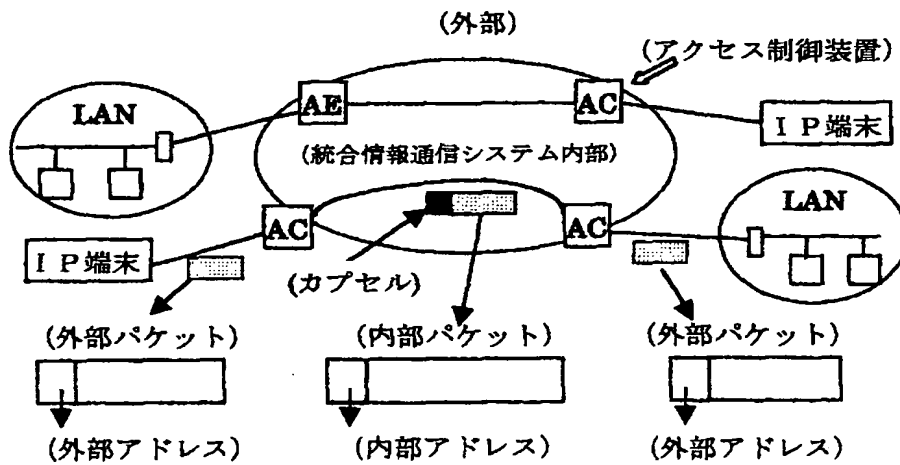
【図 1 4】



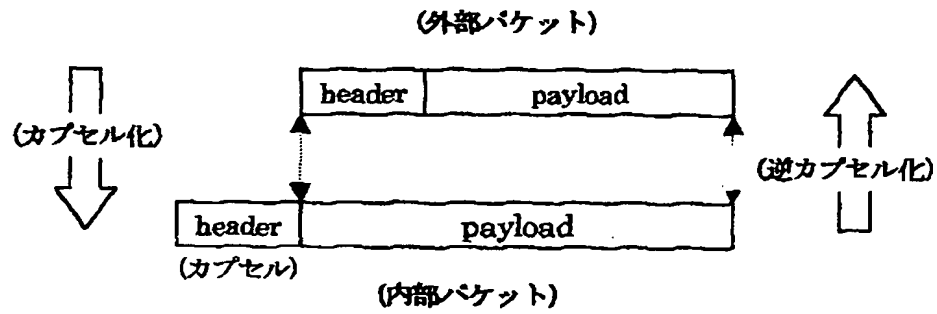
【図 1 5】



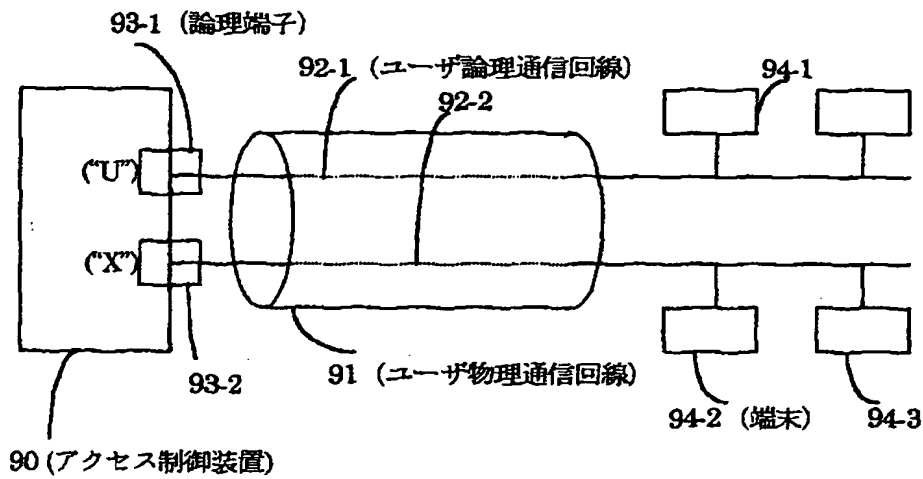
【図 1 6】



【図 1 7】



【図 1 8】



【書類名】 要約書

【要約】

【課題】 外部から運用管理サーバや中継装置へ向けて送出されてくる I P パケットを検出し、内部に侵入しないようにすることにより運用管理サーバや中継装置が不正アタックを受ける機会を減らし、通信会社網の秘密保持を守るために付与しているアドレス付与規定に違反する I P パケットを検出し廃棄することにより安全性を向上させた統合情報通信システムを提供する。

【解決手段】 統合情報通信システム内の運用管理用のサーバや中継装置に付与するアドレスは外部に対して“網外非公開アドレス”として区分し、アクセス制御装置内にパケットフィルタを設置し、通信会社管理網間の通信は境界中継装置を経由させ、境界中継装置内にパケットフィルタを設置する。アクセス制御装置内のパケットフィルタは、統合情報通信システムの外部から内部には入ってくる外部パケット内の宛先アドレスが、網外非公開アドレス範囲にあるか否かかを調べ、網外非公開アドレス範囲にある場合は前記外部パケットを廃棄する。境界中継装置内のパケットフィルタは、通信会社管理網の間を送受されるパケット内の宛先アドレスが、通信会社内部アドレス範囲にある場合は、前記パケットを廃棄する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [5 9 6 1 7 6 2 8 6]

1. 変更年月日	1 9 9 7 年 1 月 2 1 日
[変更理由]	住所変更
住 所	東京都港区赤坂7丁目3番37号
氏 名	財団法人流通システム開発センター

出 願 人 履 歴 情 報

識別番号 [3 9 8 0 0 9 3 1 7]

1. 変更年月日	1 9 9 8 年 2 月 2 日
[変更理由]	新規登録
住 所	千葉県市川市菅野 1 丁目 4 番 4 号
氏 名	有限会社宮口研究所